IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	
Motoji OHMORI et al.	:	
Serial No. NEW	:	**Attn: APPLICATION BRANCH**
Filed July 17, 2003	:	**Attorney Docket No. 2003_0831A**
SYSTEM FOR PREVENTING UNAUTHORIZED USE OF RECORDING MEDIA	:	

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-208398, filed July 17, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Motoji OHMORI et al.

By _____
Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 17, 2003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Motoji OHMORI et al. : **Attn: APPLICATION BRANCH**

Serial No. NEW : **Attorney Docket No. 2003_0831A**

Filed July 17, 2003 :

SYSTEM FOR PREVENTING UNAUTHORIZED USE OF RECORDING MEDIA :

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

COVER LETTER FOR APPLICATION FILED WITHOUT EXECUTED DECLARATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The above-identified application has been submitted without an executed oath or declaration pursuant to 37 CFR 1.41(c).

It is respectfully requested that this application be assigned a serial number and awarded a filing date pursuant to 37 CFR 1.53.

A duly executed oath or declaration pursuant to 37 CFR 1.63 will be submitted after notification by the U.S. Patent and Trademark Office pursuant to 37 CFR 1.52(d).

A non-executed copy of the Declaration and Power of Attorney, containing the inventorship information, is attached. It is respectfully requested that all communications be directed to the firm indicated on the attached Declaration and Power of Attorney, namely:

WENDEROTH, LIND & PONACK, L.L.P.
2033 K Street, N.W., Suite 800
Washington, D.C. 20006-1021

The required U.S. Patent and Trademark Office Filing Fee is submitted herewith.

Respectfully submitted,

Motoji OHMORI et al.

By _____
Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 17, 2003

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　７月１７日

出願番号
Application Number:　特願２００２－２０８３９８

[ST.10/C]:　[ＪＰ２００２－２０８３９８]

出願人
Applicant(s):　松下電器産業株式会社

２００３年　１月２１日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０００２３０

【書類名】　特許願

【整理番号】　2022540224

【提出日】　平成14年 7月17日

【あて先】　特許庁長官殿

【国際特許分類】　H04M　1/67

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　大森　基司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　上田　健一

【発明者】

【住所又は居所】　広島県東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内

【氏名】　植田　栄治

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　記録媒体不正使用防止システム

【特許請求の範囲】

【請求項１】　端末装置に着脱可能な記録媒体の不正使用防止システムであって、

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶部と、

前記第１記憶部に記憶された認証情報に対応した処理手段を記憶する第２記憶部と、

前記記録媒体の使用者が有する使用者情報と前記認証情報とを用いて認証を行う認証部と、

前記認証部の認証の内容に対応して、前記処理手段を実行する処理部と、

を備えたことを特徴とする記録媒体不正使用防止システム。

【請求項２】　前記記録媒体不正使用防止システムは、さらに前記端末装置の通信機能を使用するための通信情報を記憶する第３記憶部とを有し、

前記処理部は、前記通信情報と前記認証部の認証の内容とに対応した前記処理手段を実行することを特徴とする請求項１記載の記録媒体不正使用防止システム。

【請求項３】　前記記録媒体不正使用防止システムは、さらに前記端末装置の通信機能を使用するための通信情報を複数記憶する第４記憶部と、

前記第４記憶部の通信情報から所望の通信情報を選択する選択部とを有し、

前記処理部は、前記選択部により選択された通信情報と前記認証部の認証の内容とに対応した前記処理手段を実行することを特徴とする請求項１記載の記録媒体不正使用防止システム。

【請求項４】　前記不正使用防止システムは、さらに前記端末装置と前記記録媒体との着脱を判断する判断部を有し、

前記判断部により前記記録媒体が前記端末装置から抜き出されたことを認識した後、前記記録媒体を使用する場合には、前記認証部による認証を行うことを特徴とする請求項１乃至３記載の記録媒体不正使用防止システム。

【請求項５】　前記不正使用防止システムは、さらに前記認証情報を設定する

認証情報設定部を有し、

前記認証情報設定部により設定された認証情報を第１記憶部に記憶することを特徴とする請求項１乃至４記載の記録媒体不正使用防止システム。

【請求項６】　前記不正使用防止システムは、さらに前記処理手段を設定する処理手段設定部を有し、

前記処理手段設定部により設定された処理手段を第２記憶部に記憶することを特徴とする請求項１乃至４記載の記録媒体不正使用防止システム。

【請求項７】　前記不正使用防止システムは、さらに前記通信情報を設定する通信情報設定部を有し、

前記通信情報設定部により設定された通信情報を第３又は第４記憶部に記憶することを特徴とする請求項１乃至４記載の記録媒体不正使用防止システム。

【請求項８】　不正使用防止システムに使用する端末装置に着脱可能な記録媒体であって、

少なくとも前記記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶部と、

前記第１記憶部に記憶された認証情報に対応した処理手段を記憶する第２記憶部と、

を備えたことを特徴とする記録媒体。

【請求項９】　前記記録媒体はさらに前記端末装置の通信機能を使用するための通信情報を記憶する第３記憶部を備えたことを特徴とする請求項８記載の記録媒体。

【請求項１０】　前記記録媒体はさらに前記端末装置の通信機能を使用するための通信情報を複数記憶する第４記憶部を備えたことを特徴とする請求項８記載の記録媒体。

【請求項１１】　前記記録媒体はさらに前記記録媒体の使用者の有する使用者情報と前記認証情報とを用いて認証を行う認証部と、

を備えた請求項８乃至１０記載の記録媒体。

【請求項１２】　前記記録媒体はさらに前記端末装置と前記記録媒体との着脱を判断する判断部を有し、

前記判断部により前記記録媒体が前記端末装置から抜き出されたことを認識した後、前記記録媒体を使用する場合には、前記認証部による認証を行うことを特徴とする請求項８乃至１１記載の記録媒体不正使用防止システム。

【請求項１３】　不正使用防止システムに使用する記録媒体が着脱可能な端末装置であって、

少なくとも前記記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶部と、

前記第１記憶部に記憶された認証情報に対応した処理手段を記憶する第２記憶部と、

前記端末装置の使用者の有する端末使用者情報と前記認証情報とを用いて認証を行う認証部と、

前記認証部の認証の内容に対応して前記処理手段を実行する処理部と、

を備えたことを特徴とする端末装置。

【請求項１４】　前記端末装置は、さらに前記端末装置の通信機能を使用するための通信情報を複数記憶する第４記憶部と、

前記第４記憶部の使用者識別情報から所望の使用者識別情報を選択する選択部とを有し、

前記処理部は、前記選択部により選択された通信情報と前記認証部の認証の内容に対応し前記処理手段を実行することを特徴とする請求項１３記載の端末装置。

【請求項１５】　端末装置に着脱可能な記録媒体の不正使用防止方法であって、

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶工程と、

前記第１記憶工程に記憶された認証情報に対応した処理手段を記憶する第２記憶工程と、

前記記録媒体の使用者が有する使用者情報と前記認証情報とを用いて認証を行う認証工程と、

前記認証工程の認証の内容に対応して、前記処理手段を実行する処理工程と、

を備えたことを特徴とする記録媒体不正使用防止方法。

【請求項１６】　端末装置に着脱可能な記録媒体の不正使用防止方法であって、

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶工程と、

前記第１記憶工程に記憶された認証情報に対応した処理手段を記憶する第２記憶工程と、

前記端末装置の通信機能を使用するための通信情報を記憶する第３記憶工程と、

前記記録媒体の使用者が有する使用者情報と前記認証情報とを用いて認証を行う認証工程と、

前記通信情報と前記認証工程の認証の内容とに対応した前記処理手段を実行する処理工程と、

を備えたことを特徴とする記録媒体不正使用防止方法。

【請求項１７】　端末装置に着脱可能な記録媒体の不正使用防止方法であって、

前記記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶工程と、

前記第１記憶工程に記憶された認証情報に対応した処理手段を記憶する第２記憶工程と、

前記端末装置の通信機能を使用するための通信情報を複数記憶する第４記憶工程と、

前記第４記憶工程の通信情報から所望の通信情報を選択する選択工程と、

前記記録媒体の使用者が有する使用者情報と前記認証情報とを用いて認証を行う認証工程と、

前記選択工程により選択された通信情報と前記認証工程の認証の内容とに対応した前記処理手段を実行する処理工程と、

を備えたことを特徴とする記録媒体不正使用防止方法。

【請求項１８】　請求項１５から１７の何れか一つに記載の方法を実行する記

録媒体不正使用防止プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、端末装置に対して着脱可能な記録媒体の不正使用防止に関するものである。

【０００２】

【従来の技術】

携帯電話等の電子機器の分野において、近年、ＳＩＭ（Subscriber Identity Module）カードと称される利用者識別カードを、電話機本体に装着して通信を行い得るようにするシステムが考えられている。そして、このＳＩＭカードには、ＳＩＭカードの所有者の個人情報が記憶されている。このような構成とすることにより、電話機を所有しない者、あるいは自らの電話機が故障、電池切れ等で使用不能となった場合でも、他者の電話機あるいは公共の電話機を用いて、自己のＳＩＭカードを装着することにより、使用者自身のＩＤコードを用いた通話を行うことができる。これにより、課金処理もＳＩＭカードの所有者を対象として行うことができるようになる。さらに、自らの所有する電話機ではない場合でも、ＳＩＭカードに記憶されたメモリダイヤルのデータに基づいて電話をかけることも可能になる。

【０００３】

【発明が解決しようとする課題】

しかしながら、このような便利なＳＩＭカードであっても、紛失又は盗難等によりＳＩＭカードが意図せず第三者に渡ってしまうことが考えられる。このような場合、そのＳＩＭカードを取得した第三者の悪意により不正な使用がなされることも考えられる。

【０００４】

また、一個人が複数のSIMカードを携帯する可能性も考えられ、紛失又は盗難による不正使用の可能性が高くなることも予想される。

【０００５】

さらに、ＳＩＭカードのような携帯電話に着脱可能な記録媒体が、上述した通信機能に加えて、例えば、電子商取引等の機能を有することも考えられる。そのような場合には、紛失又は盗難による第三者の使用により、上述した記録媒体の所有者が、電子マネーが第三者により使用されることなどにより、さらに記録媒体の使用者が深刻な事態に陥ることが予想される。

【０００６】

本発明は、上記問題点を解決することによって、第三者の不正使用を防止し、記録媒体の所有者に安全且つ利便性の高い記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】

上記の目的を達成するために、この発明の端末装置に着脱可能な記録媒体の不正使用防止システムは、前記記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶部と、前記第１記憶部に記憶された認証情報に対応した処理手段を記憶する第２記憶部と、前記記録媒体の使用者が有する使用者情報と前記認証情報とを用いて認証を行う認証部と、前記認証部の認証の内容に対応して、前記処理手段を実行する処理部と、を含むことを特徴とする。これにより、処理手段の内容に対応して適切に第三者の使用を防止することが可能になる。

【０００８】

また、前記不正使用防止システムは、さらに前記端末装置を使用するための通信情報を複数記憶する第４記憶部と、前記第４記憶部の通信情報から所望の通信情報を選択する選択部とを有し、前記処理部は、前記選択部により選択された通信情報と前記認証部の認証の内容とに対応した前記処理手段を実行する構成としてもよい。これにより、一個人が複数の電話番号を有する場合であっても、SIMカードのような記録媒体を複数携帯する必要がなく、記録媒体の利便性を向上させることができる。

【０００９】

また、前記不正使用防止システムは、さらに前記端末装置と前記記録媒体の着脱を判断する判断部を有し、前記判断部により前記記録媒体が前記端末装置から

抜き出されたことを認識した後、前記記録媒体を使用する場合には、前記認証部による認証を行う構成としてもよい。これにより、第三者により記録媒体が前記端末装置から抜き出された場合であっても再度認証部による認証を行うため、第三者の不正使用を防止することが可能になる。

【００１０】

【発明の実施の形態】

図１は、この発明の一実施の形態に係る端末装置から着脱可能な記録媒体の不正使用防止システム（以下、「記録媒体不正使用防止システム」とする。）の概略構成図である。

【００１１】

この実施の形態の記録媒体不正使用防止システムは、端末装置１００又は２００と、端末装置１００又は２００から着脱可能な記録媒体３００とを備えている。

【００１２】

端末装置１００又は２００は、携帯型の電話機、PDA (Personal Digital Assistant)、パーソナルコンピュータ、カーナビゲーションシステム、FAX、デジタルカメラ（PDA、パーソナルコンピュータ、カーナビゲーションシステム、FAX、デジタルカメラは図示せず）等、記録媒体３００が着脱可能な装置である。

【００１３】

記録媒体３００は、以下に述べる処理が可能であり、端末装置１００又は２００に着脱可能な記録媒体であれば特に限定されるものではない。

【００１４】

図２は、図１に示した端末装置１００又は２００の概略構成を示すブロック図である。

【００１５】

端末装置１００又は２００は、出力部２０２と、入力部２０４と、送受信部２０６と、メモリ２０８と、記録媒体制御部２１２と、制御部２１４と、により構成されており、各部はバス２１６によって接続されている。

【００１６】

出力部２０２は、液晶表示装置等により構成されており、制御部２１４から出力命令されたデータを表示する。

【００１７】

入力部２０４は、タッチパネル、または数字入力キーなどの入力機能を備えたキーボード等により構成されており、タッチパネルで押下された位置の座標情報、またはキーボード等のキー操作信号を制御部２１４に出力する。

【００１８】

送受信部２０６は、アンテナ等が接続されており、制御部２１４の制御により外部から信号を受信又は外部へ信号を送信する。

【００１９】

メモリ２０８は、入力部２０４により入力された入力指示及び制御部２１４によりなされた処理内容を一時格納するデータ格納機能と、制御部２１４により実行される各種処理プログラムや各種アプリケーションプログラムを格納するプログラム管理機能とにより構成されている。

【００２０】

記録媒体制御部２１２は、端末装置１００又は２００に装備されているスロット（図示せず）に記録媒体３００が差し込まれることにより、インターフェース２１８を介して記録媒体３００の利用を制御する。

【００２１】

制御部２１４は、上述した出力部２０２、入力部２０４、送受信部２０６、メモリ２０８、記録媒体制御部２１２に接続されており、上述した各部の制御を行う。この制御部２１４及びその各部は、例えばROMやRAM等のコンピュータ読み取り可能な記録媒体（図示せず）に格納されたプログラムをCPU（Central Processing Unit）が読み取って実行することによって具現化される。

【００２２】

以上のような端末装置１００又は２００に対して着脱可能な記録媒体３００の第一実施形態について図３から図６を参照して説明する。

【００２３】

図３は、記録媒体３００の第一実施形態である記録媒体３００Aのブロック図

である。

【００２４】

記録媒体３００Aは、認証情報設定部３２０と処理手段設定部３２２からなる設定部３０３と、第１記憶部３０６と第２記憶部３１４からなる記憶部３０５と、受付部３０９と、認証部３１２と処理部３１５からなる制御部３０８と、を備えている。

【００２５】

受付部３０９は、記録媒体３００Aに入力された使用者情報を受付ける。使用者情報とは、具体的には、１以上の数字又はアルファベット等の組合せ、指紋情報、声紋情報、虹彩情報、輪郭情報及びDNA情報などの記録媒体３００Aの使用者が有する情報である。この入力情報は、端末装置１００又は２００を利用して入力してもよいし、記録媒体３００A自体に入力機能を設けて入力する構成としてもよい。

【００２６】

次に、第１記憶部３０６と第２記憶部３１４に格納される情報について、図４を参照して詳細に説明する。

【００２７】

第１記憶部３０６は、記録媒体３００Aの使用の可否を決定する複数の認証情報を記憶している。また、この認証情報は、後述する第２記憶部３１４に格納されている処理手段に関する情報にも対応している。具体的には、この認証情報は、１以上の数字又はアルファベット等の組合せ、指紋情報、声紋情報、虹彩情報、輪郭情報及びDNA情報などにより実現可能となる。また、認証情報はこれらの複数の組合せとすることも可能である。これにより、後述する処理手段の内容に対応して、高度な認証を行うことが可能になる。

【００２８】

第２記憶部３１４は、第１記憶部３０６の複数の認証情報に対応し、後述する処理手段に関する情報を格納している。処理手段とは、記録媒体３００Aのメモリ（図示せず）に記憶したデータへのアクセス、ゲーム機能などである。ここで、記憶したデータに複数の領域（メモリA、メモリBなど）を設け、記憶したデー

タの内容に応じた認証情報を設定することも可能である。なお、第２記憶部３１４は、端末１００又は２００側に設けることも装置可能である。

【００２９】

設定部３０３は、認証情報設定部３２０と処理手段設定部３２２とによって構成されている。認証情報設定部３２０は第１記憶部３０６の認証情報を設定する。処理手段設定部３２２は第２記憶部３１４の処理手段を設定する。なお、設定部３０３が行う設定は、外部の装置を用いて設定することも可能である。

【００３０】

次に、認証部３１２は、上述した受付部３０９から得られる使用者情報３１０と上述した第１記憶部３０６に記憶された認証情報３１３との認証を行う。なお、認証部３１２は、端末装置１００又は２００側に設けることも可能である。

【００３１】

処理部３１５は、上述した認証部３１２の認証の内容に応じて、第２記憶部の処理手段の内容を実行する。なお、処理部３１５は、端末装置１００又は２００側に設けることも可能である。

【００３２】

以上のような構成において、入力された使用者情報と認証情報との認証を行い、認証が可能な場合に、認証情報に対応する予め設定された処理手段を実行する第一実施形態の動作について図５から図６を参照して説明する。

【００３３】

図５は、記録媒体３００Aの設定部３０３により第１記憶部の認証情報及び第２記憶部の処理手段を設定するフローチャートである。この処理において、まず、設定部３０３の認証情報設定部３２０は第１記憶部の認証情報を設定する（S1）。次に、設定部３０３の処理手段設定部３２２は、設定した認証情報に対応した処理手段を設定する（S2）。なお、この処理は、先に処理手段を設定し、その後処理手段に対応した認証情報を設定する手順とすることも可能である。

【００３４】

図６は、記録媒体３００Aの処理手順を示すフローチャートである。まず、受付部３０９が記録媒体３００Aの使用者情報を受付ける（S11）。次に、認証部

３１２において、第１記憶部に記憶された認証情報と使用者情報とが一致するか否かを認証する（Ｓ１２）。認証情報と使用者情報とが一致する場合には、処理部３１５は、第２記憶部に設定された認証情報に対応した処理手段を実行する（Ｓ１３）。ここで、図４を参照しながら、処理手段と認証情報の対応について説明する。例えば、使用者がPW３と同様の内容の使用者情報を入力した場合は、メモリAとメモリBの使用が可能になる。一方、使用者がPW2と同様の内容の使用者情報を入力した場合は、メモリAとゲームの使用が可能になる。ここで、メモリAとメモリBには重要度が異なる情報を記憶することにより、情報の重要度に対応した認証情報を設定することが可能になる。一方、認証情報と使用者情報とが一致しない場合には、使用者が入力した使用者情報が第１記憶部の認証情報と一致しない旨を出力する（Ｓ１４）。さらに、第１記憶部の認証情報から、認証情報の不要な処理手段の有無を検索する（Ｓ１５）。認証情報の不要な処理手段とは、図４においては、認証情報なしに対応するメモリAの使用を可能にする処理手段に該当する。ここで、認証情報の不要な処理手段がある場合には、対応する第２記憶部の処理手段を実行する（Ｓ１６）。一方、認証情報の不要な処理手段がない場合には、そのまま終了する。認証情報の不要な処理手段とは、認証情報を設定する必要のない処理手段をいう。なお、ステップ１４からステップ１６は、必須ではなく省略することも可能である。

【００３５】

次に、端末装置１００又は２００に対して着脱可能な記録媒体３００の第二実施形態について図７から図９を参照して説明する。

【００３６】

図７は、記録媒体３００の第二実施形態である記録媒体３００Bのブロック図である。

【００３７】

第二実施形態は第一実施形態である３００Aに加えて、第３記憶部４０２若しくは第４記憶部４０５と、選択部４０８と、通信情報設定部４１０とを有する。第一実施形態において説明した内容については、説明が重複するため省略する。

【００３８】

第３記憶部４０２又は第４記憶部４０５に格納される情報について、図８又図９を参照して詳細に説明する。

【００３９】

第３記憶部４０２は、図８に示すように、第１記憶部３０６・第２記憶部３１４に対応した、端末装置１００又は２００の通信機能を使用するための通信情報を記憶する。ここで、通信情報とは、例えば、電話番号をある関数で変換した情報などである。これによって、第三者が第３記憶部の情報を取得した場合であっても、容易に電話番号を認識することができず、第三者の不正使用の防止を図ることができる。ある関数は、端末装置に対して、通信情報を利用して通信機能を提供する業者が保持することも可能である。また、上述した電話番号をある関数で変換した情報以外にも、通信情報の保有者が予め自己の認識しうる情報に変更しておくことも可能である。この場合であっても、第三者の不正使用の防止を図ることができる。

【００４０】

第４記憶部４０５は、図９に示すように、上述した通信情報を複数記憶する。これにより、一個人が複数の通信情報を必要とする場合であっても、複数の通信情報を一つの記録媒体に記憶することが可能になり、利便性を向上させることができる。以下、この第二実施形態では、第４記憶部を用いて説明する。

【００４１】

次に、選択部４０８は、上述した第４記憶部４０５から所望の通信情報を選択する。但し、この選択部４０８は、端末装置１００又は２００若しくは外部の装置を用いて行うことも可能である。

【００４２】

通信情報設定部４１０は、上述した第３記憶部４０２若しくは第４記憶部４０５に所望の通信情報を設定する。これにより、新しい通信情報が必要になった場合又は第４記憶部に記憶された通信情報が不要になった場合に第４記憶部の設定内容を変更することが可能になる。

【００４３】

以上のような構成において、所望の通信情報を選択し、入力された認証情報と

選択された通信情報に対応する処理手段を実行する第二実施形態の動作について図１０から図１１を参照して説明する。

【００４４】

図１０は、記録媒体３００Bの設定部３０３により、第１記憶部３０６の認証情報、第２記憶部３１４の処理手段、第３記憶部４０２又は第４記憶部の通信情報を設定するフローチャートである。この処理において、まず、設定部３０３の通信情報設定部４１０は、第３記憶部４０２又は第４記憶部４０５に一つ又は少なくとも一つ以上の通信情報を設定する（Ｓ２１）。次に、第３記憶部４０２又は第４記憶部４０５に対応して、設定部３０３の認証情報設定部３２０は、第１記憶部３０６の認証情報を設定する（Ｓ２２）。次に、設定部３０３の処理手段設定部３２２は、設定した通信情報と認証情報に対応した処理手段を設定する（Ｓ２３）。なお、第１記憶部３０６の認証情報と第２記憶部３１４の処理手段と、第３記憶部４０２又は第４記憶部４０５の通信情報の設定は、どのような順番で設定することも可能である。

【００４５】

ここで、第２記憶部に記憶される処理手段の内容について詳細に説明する。処理手段は、通信機能、電子商取引機能、電子財布機能、メモリ機能、ナビゲーションシステム機能等により構成される。

【００４６】

また、通信機能においては、通話機能、電子メール機能又は着信機能のみなどを選択することも可能であり、機能の内容に対応した認証情報を設定することも可能である。また、通信機能を使用する際には、通話機能の課金に上限を設け、その上限に対応した認証情報を設定することも可能である。

【００４７】

また、電子商取引機能においても、電子商取引の対象や金額の設定に応じて認証情報を設定することも可能である。

【００４８】

また、電子財布機能においては、預金、残高照会、引き落としなどの機能に応じた認証情報を設定することも可能である。

【００４９】

また、メモリ機能においては、通信機能を利用して取得した情報を、情報の重要度に応じて認証情報を設定することも可能である。

【００５０】

図１１は、記録媒体３００Bの処理手順を示すフローチャートである。

【００５１】

まず、選択部４０８は、第４記憶部４０５に記憶された通信情報から所望の通信情報を選択する（Ｓ３１）。次に、受付部３０９が記録媒体３００Bの使用者情報を受付ける（Ｓ３２）。次に、認証部３１２において、第１記憶部３０６に記憶された認証情報と使用者情報とが一致するか否かを認証する（Ｓ３３）。認証情報と使用者情報とが一致する場合には、選択部４０８により選択された通信情報と認証部３１２により認証された認証情報に対応した第２記憶部３１４に記憶された処理手段の実行を可能にする（Ｓ３４）。ここで、図９を参照しながら、処理手段の実行内容について説明する。例えば、使用者が法人の通信情報を選択し、さらにPW１と同様の内容の使用者情報を入力した場合は、端末装置１００又は２００の通信機能を実行可能にする処理を行う。さらに、使用者が上記通信機能に加えて、電子商取引の機能を実行可能にするためには、使用者がPW１の代わりにPW２を使用者情報として入力するという簡単な手段で電子商取引の機能を実行可能にすることができる。なお、図９においては、それぞれ異なる認証情報を設定したが、使用者の要望に応じて、同じ認証情報を設定することも可能である。一方、認証情報と使用者情報とが一致しない場合には、認証情報と使用者情報が一致しない旨を出力する（Ｓ３５）。さらに、第１記憶部の認証情報から、認証情報の不要な処理手段の有無を検索する（Ｓ３６）。ここで、認証情報の不要な処理手段がある場合には、対応する第２記憶部の処理手段を実行する（Ｓ３７）。認証情報の不要な処理手段とは、図９においては、法人の通信情報を選択した場合には、認証情報なしに対応するメモリＢの使用を可能にする処理手段に該当する。一方、認証情報の不要な処理手段がない場合には、そのまま終了する。なお、ステップ５からステップ８は必須ではなく、省略することも可能である。

【００５２】

次に、端末装置１００又は２００に対して着脱可能な記録媒体３００の第三実施形態について図１２から図１３を参照して説明する。

【００５３】

図１２は、記録媒体３００の第三実施形態である記録媒体３００Cのブロック図である。

【００５４】

第三実施形態は第一実施形態である３００A又は第二実施形態である３００Bに加えて、判断部６０２を有する。第一実施形態又は第二実施形態において説明した内容については、説明が重複するため省略する。

【００５５】

判断部６０２は、着脱検出信号INS６０４を利用して、端末装置１００又は２００と記録媒体３００Cの着脱を検出する。

【００５６】

着脱検出信号ＩＮＳ６０４の信号線の一端は記録媒体内部ではグランドＶｓｓ６０６に接続されている。そして着脱検出信号ＩＮＳ６０４の信号線の他端は、この記録媒体３００Cに装着される端末装置１００又は２００において、プルアップ抵抗Ｒ６０５を介し端末装置内の電源に接続されている。さらに、グランドＶｓｓ６０６の信号線は、この記録媒体が挿入される端末装置１００又は２００内のグランドに接続されるように構成されている。この構成により、端末装置１００又は２００の電源電圧Ｖｄｄ６０３を利用して記録媒体３００Cが装着される端末装置１００又は２００からの着脱状態を検出することが可能になる。

【００５７】

以上のような構成において、端末装置が記録媒体から抜き出されたことを認識した後、記録媒体を使用する場合に、認証を行うことにより記録媒体の不正使用を防止する第三実施形態の動作について図１３から図１４を参照して説明する。

【００５８】

図１３は、端末装置１００又は２００から記録媒体３００Cの着脱を検出する処理を示すフローチャートである。この処理において、まず、検出部５２２は、着脱検出信号INS５０４を受信することにより端末装置１００又は２００から記

録媒体３００Cを着脱したことを検出する（S４１）。次に、コントローラ５２６は、検出部５２２が着脱検出信号INS５０４を受信したことを履歴情報記録部５２８に送信する（S４２）。次に、履歴情報記録部５２８は、履歴情報５２４として着脱検出信号INS５０４を記録する（S４３）。この履歴情報５２４としては、端末装置１００又は２００から記録媒体３００が抜き出されたという情報に加えて、記録媒体３００Cが着脱された時間、記録媒体３００Cが着脱された場所等の情報であってもよい。

【００５９】

図１４は、記録媒体３００Cの処理手順を示すフローチャートである。まず、記録媒体３００Cの履歴情報記録部６２８に履歴情報６２４が記録されているか否かを検出する（S５１）。履歴情報が記録されている場合には、記録媒体３００Cは、パスワード等の入力を要求する（S５２）。次に、選択部４０８は、第４記憶部に記憶された通信情報から所望の通信情報を選択する（S５３）。次に、受付部３０９が記録媒体３００Cの使用者情報を受信する（S５４）。次に、認証部３１２において、第１記憶部に記憶された認証情報と使用者情報とが一致するか否かを認証する（S５５）。認証情報と使用者情報とが一致する場合には、選択部４０８により選択された通信情報と認証部３１２により認証がなされた認証情報に対応した第２記憶部に記憶された処理手段の実行を可能にする（S５６）。

【００６０】

一方、認証情報と使用者情報とが一致しない場合には、認証情報と使用者情報が一致しない旨を出力する（S５７）。さらに、第１記憶部と第２記憶部から、認証情報の不要な処理手段の有無を検索する（S５８）。ここで、認証情報の不要な処理手段がある場合には、その処理手段を実行する（S５９）。一方、認証情報の不要な処理手段がない場合には、そのまま終了する。なお、ステップ５７からステップ５９は必須ではなく、省略することも可能である。

【００６１】

【発明の効果】

以上説明したように、この発明によれば、処理手段の内容に対応した認証情報

を設定することが可能になるため、効率良く処理手段の内容に対応して効率良く第三者の使用を防止することが可能になる。

【００６２】

また、一つの記録媒体に複数の通信情報を複数記憶するため、一個人が複数の通信情報を有する場合であっても、複数の記録媒体を携帯する必要がなく、紛失又は盗難による不正使用の可能性を低くすることができる。

【００６３】

また、端末装置が記録媒体が着脱された後、記録媒体が使用される場合には、必ず認証が行われるため、第三者により記録媒体が端末装置から抜き出された場合であっても再度認証を行うため、不正使用を防止することが可能になる。

【図面の簡単な説明】

【図１】

この発明の一実施の形態に係る端末装置から着脱可能な記録媒体の不正使用防止システムの概略構成を示す図

【図２】

端末装置の概略構成を示す図

【図３】

第一実施形態に係る記録媒体の概略構成を示すブロック図

【図４】

第一実施形態に係る第１、２記憶部の内容を説明する図

【図５】

第一実施形態に係る設定部の処理手順を設定するフローチャート

【図６】

第一実施形態に係る記録媒体の処理手順を説明するフローチャート

【図７】

第二実施形態に係る記録媒体の概略構成を示すブロック図

【図８】

第二実施形態に係る第１、２、３記憶部の内容を説明する図

【図９】

第二実施形態に係る第１、２、４記憶部の内容を説明する図

【図１０】

第二実施形態に係る設定部の処理手順を設定するフローチャート

【図１１】

第二実施形態に係る記録媒体の処理手順を説明するフローチャート

【図１２】

第三実施形態に係る記録媒体の概略構成を示すブロック図

【図１３】

端末装置と記録媒体との着脱を検出する処理を示すフローチャート

【図１４】

第三実施形態に係る記録媒体の処理手順を説明するフローチャート

【符号の説明】

１００，２００　端末装置

３０６　第１記憶部

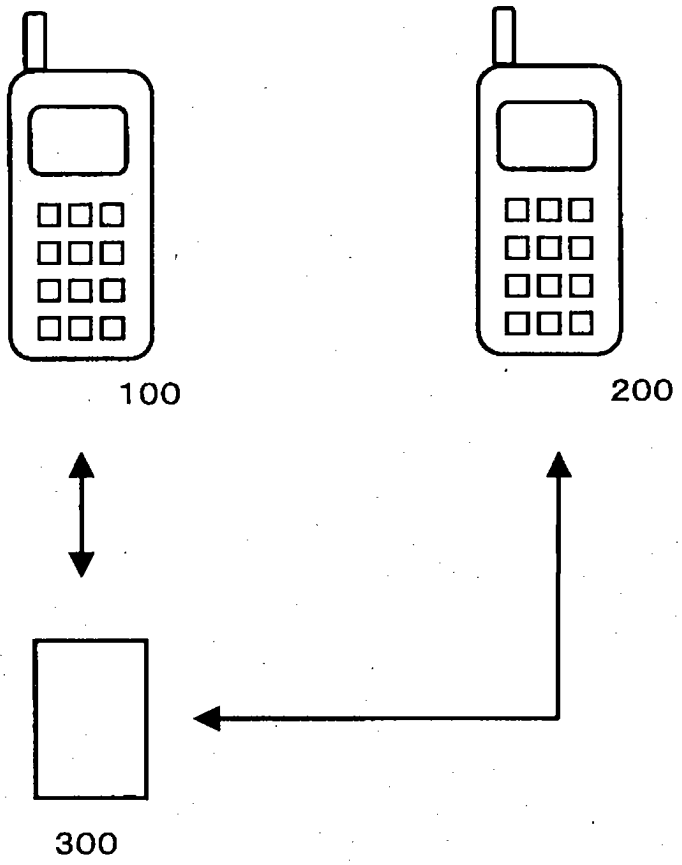
３１２　認証部

３１４　第２記憶部

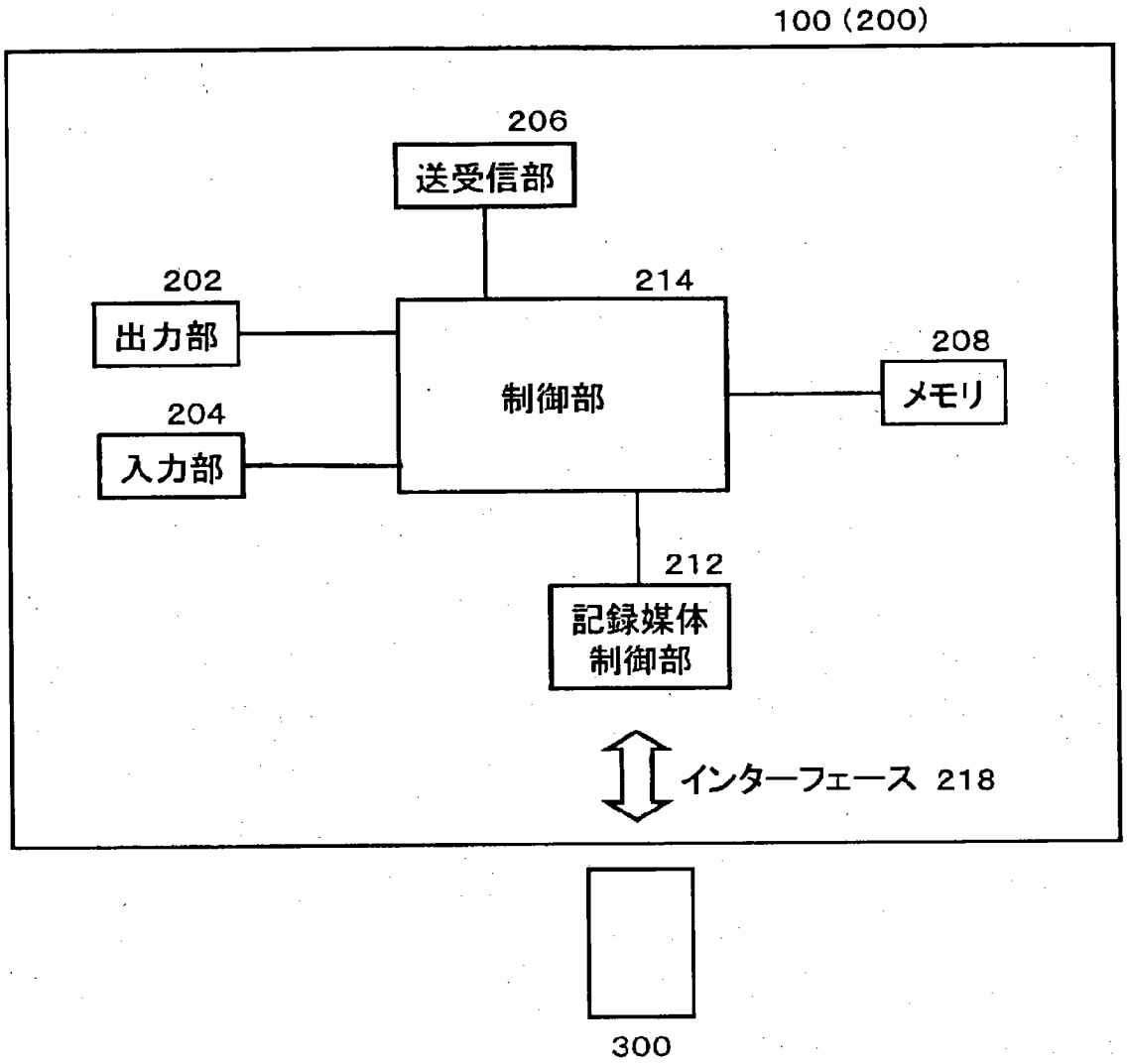
３１５　処理部

【書類名】　　図面

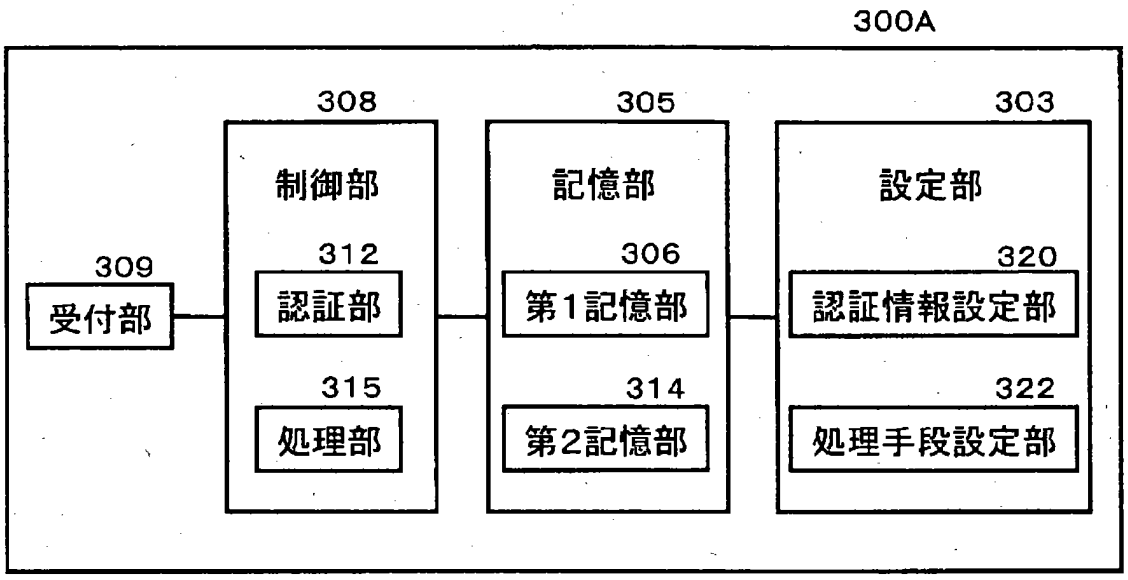
【図１】



【図２】


100 (200)
206
送受信部
202
出力部
214
制御部
208
メモリ
204
入力部
212
記録媒体
制御部
インターフェース 218
300

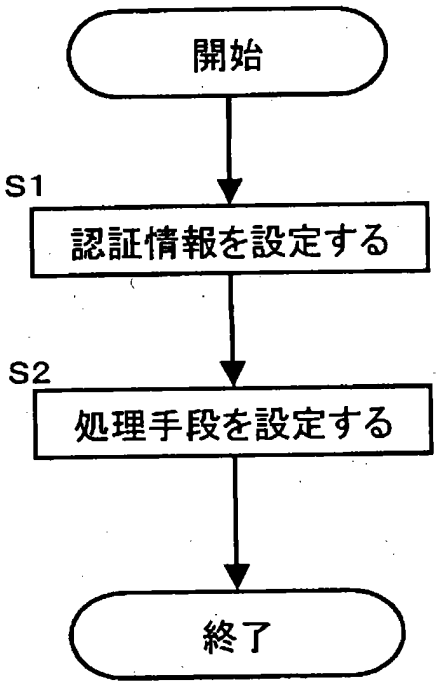
【図３】



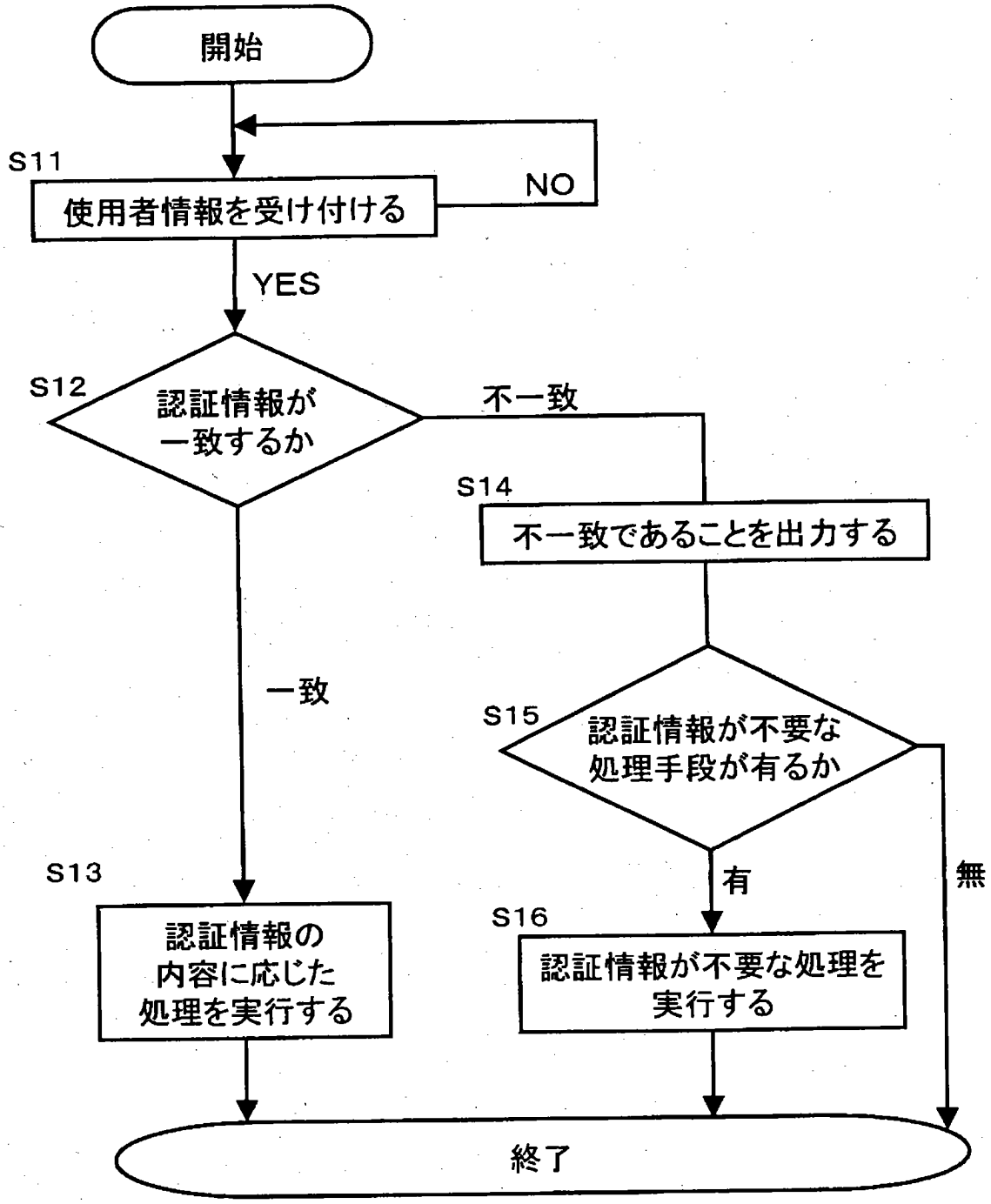
【図４】

第1記憶部	第2記憶部
認証情報	処理手段
なし	メモリ A
PW1	メモリ A+B
PW2	メモリ A, ゲーム
PW3	メモリ A+B, ゲーム

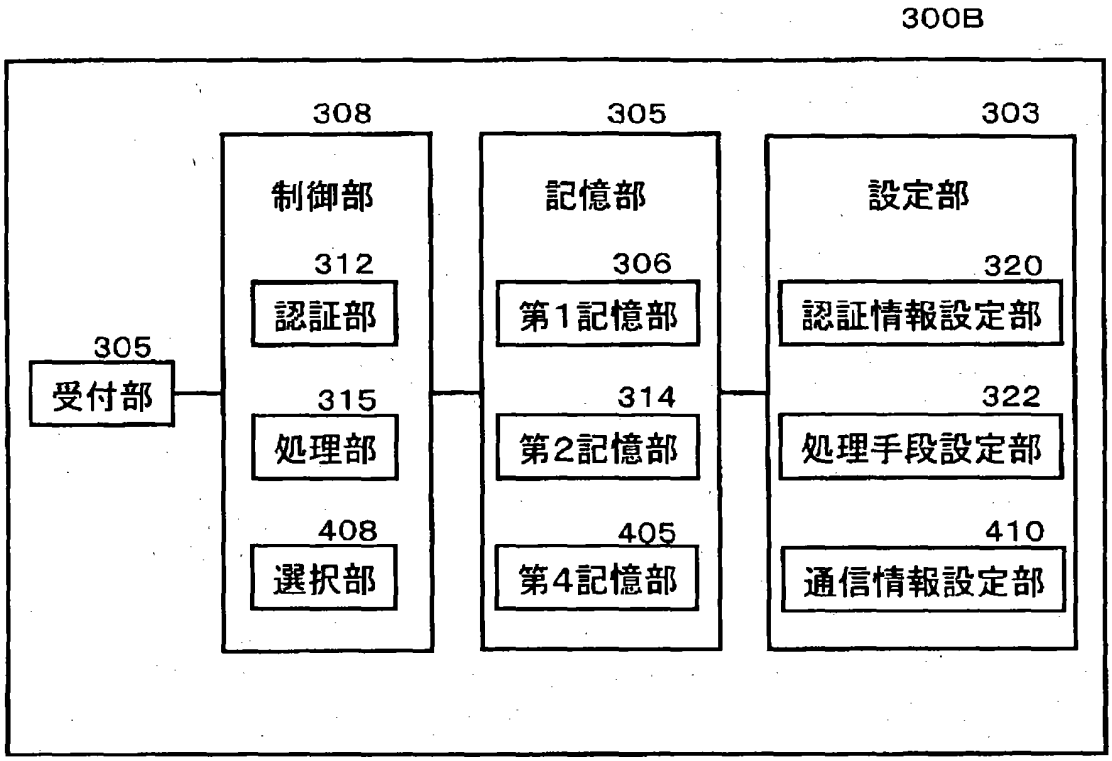
【図５】



【図６】


開始
S11
使用者情報を受け付ける
NO
YES
S12
認証情報が
一致するか
不一致
S14
不一致であることを出力する
一致
S15
認証情報が不要な
処理手段が有るか
有
無
S13
認証情報の
内容に応じた
処理を実行する
S16
認証情報が不要な処理を
実行する
終了

【図７】



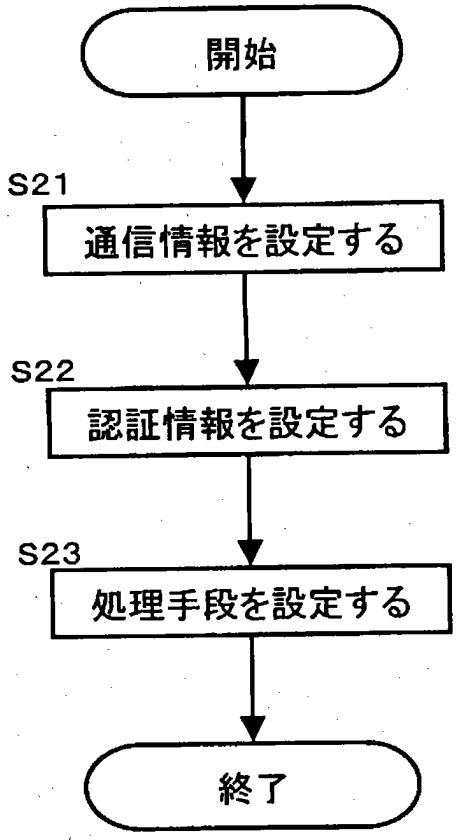
【図８】

第3記憶部	第1記憶部	第2記憶部
通信情報	認証情報	処理手段
○○○	なし	メモリ A
－○○○○	PW1	メモリ A＋B
－○○○○	PW2	メモリ A＋B，通信機能
	PW3	メモリ A＋B，通信機能，電子商取引

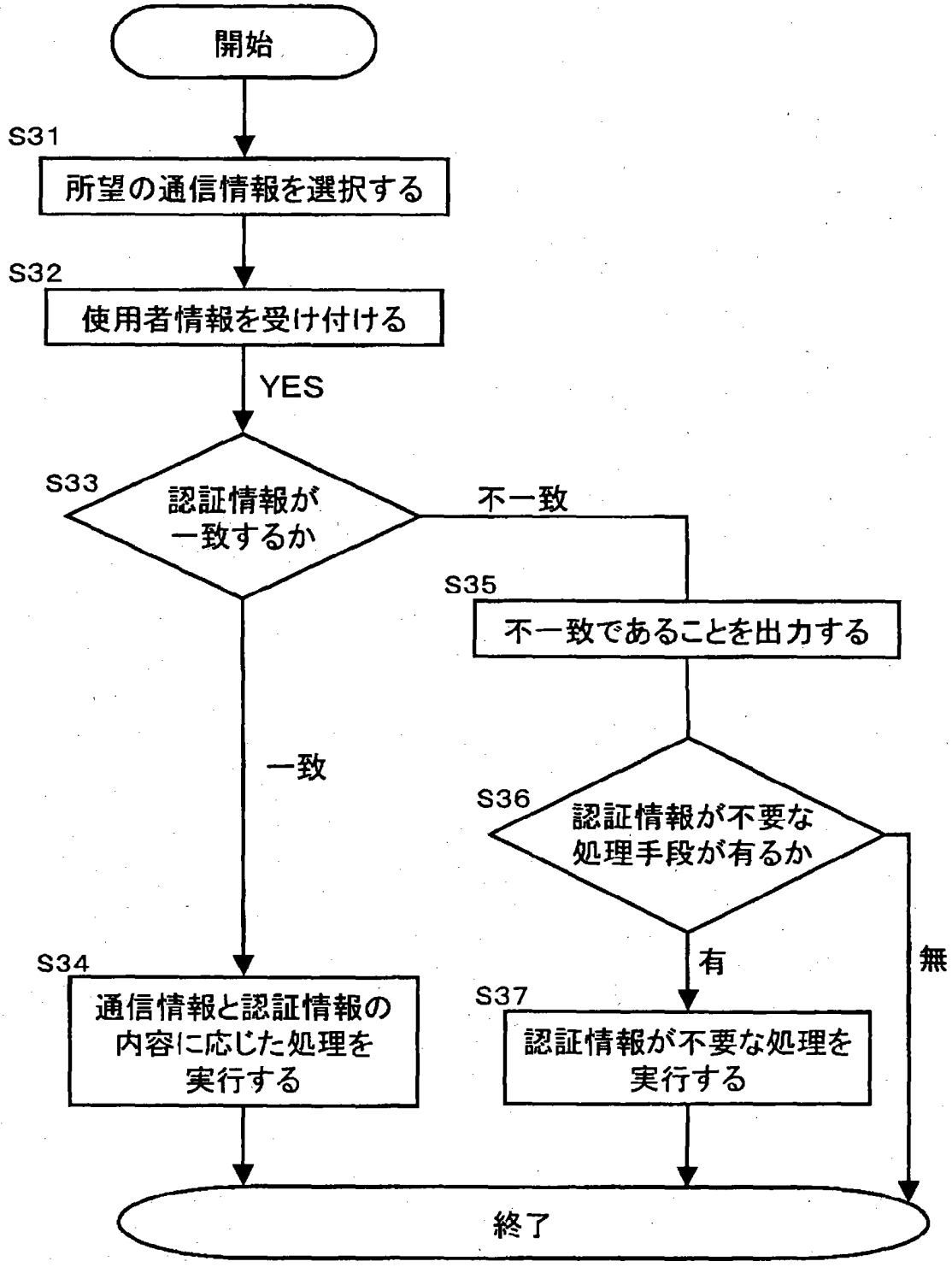
【図９】

第4記憶部	第1記憶部	第2記憶部
通信情報	認証情報	処理手段
○○○－○○○－○○○○ （法人）	PW1	通信機能
	PW2	通信機能 ＋ 電子商取引
	なし	メモリ B
△△△－△△△－△△△△ （個人1）	PW3	メモリ A ＋ メモリ B
	PW4	メモリA，B ＋ 通信機能
×××－×××－×××× （個人2）	PW5	通信機能
	なし	メモリ A

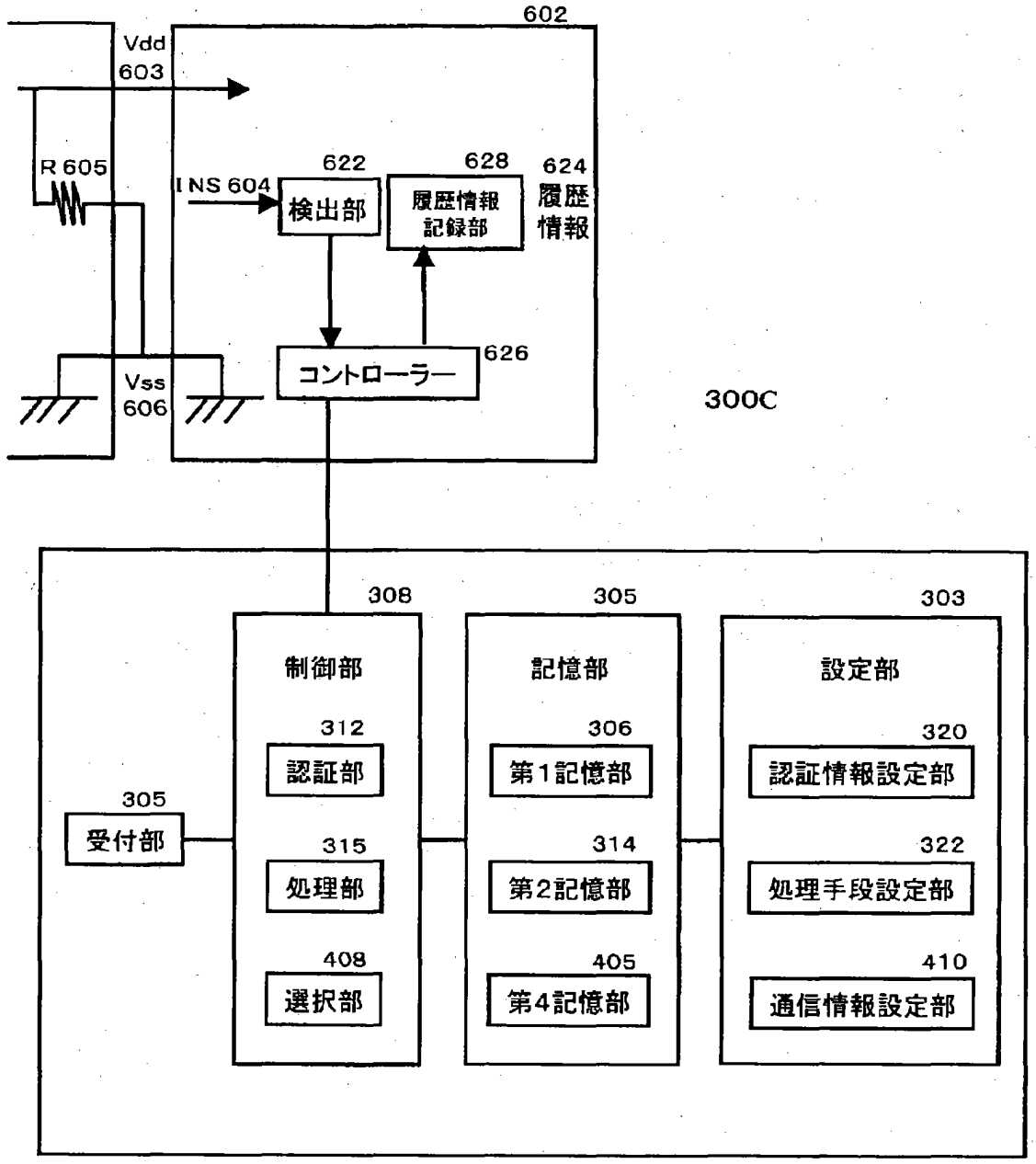
【図１０】



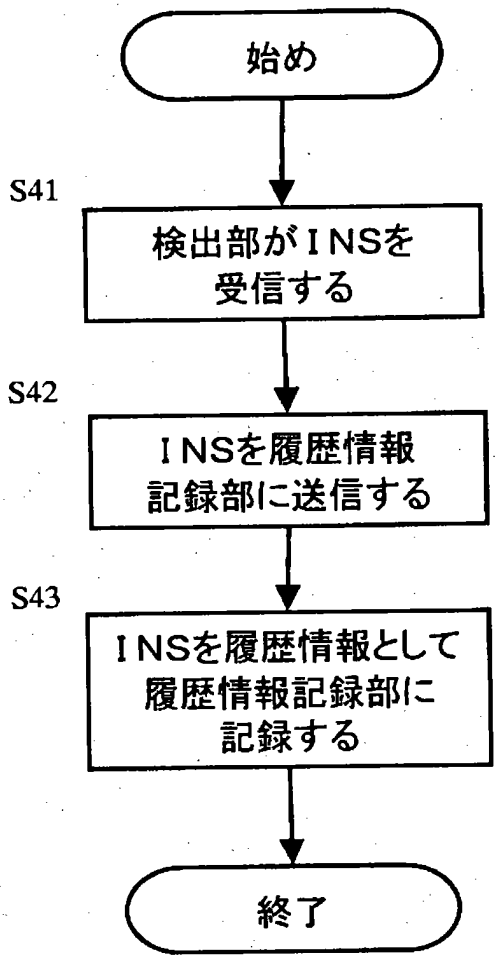
【図１１】


開始
S31
所望の通信情報を選択する
S32
使用者情報を受け付ける
YES
S33
認証情報が
一致するか
不一致
S35
不一致であることを出力する
一致
S36
認証情報が不要な
処理手段が有るか
有
無
S34
通信情報と認証情報の
内容に応じた処理を
実行する
S37
認証情報が不要な処理を
実行する
終了

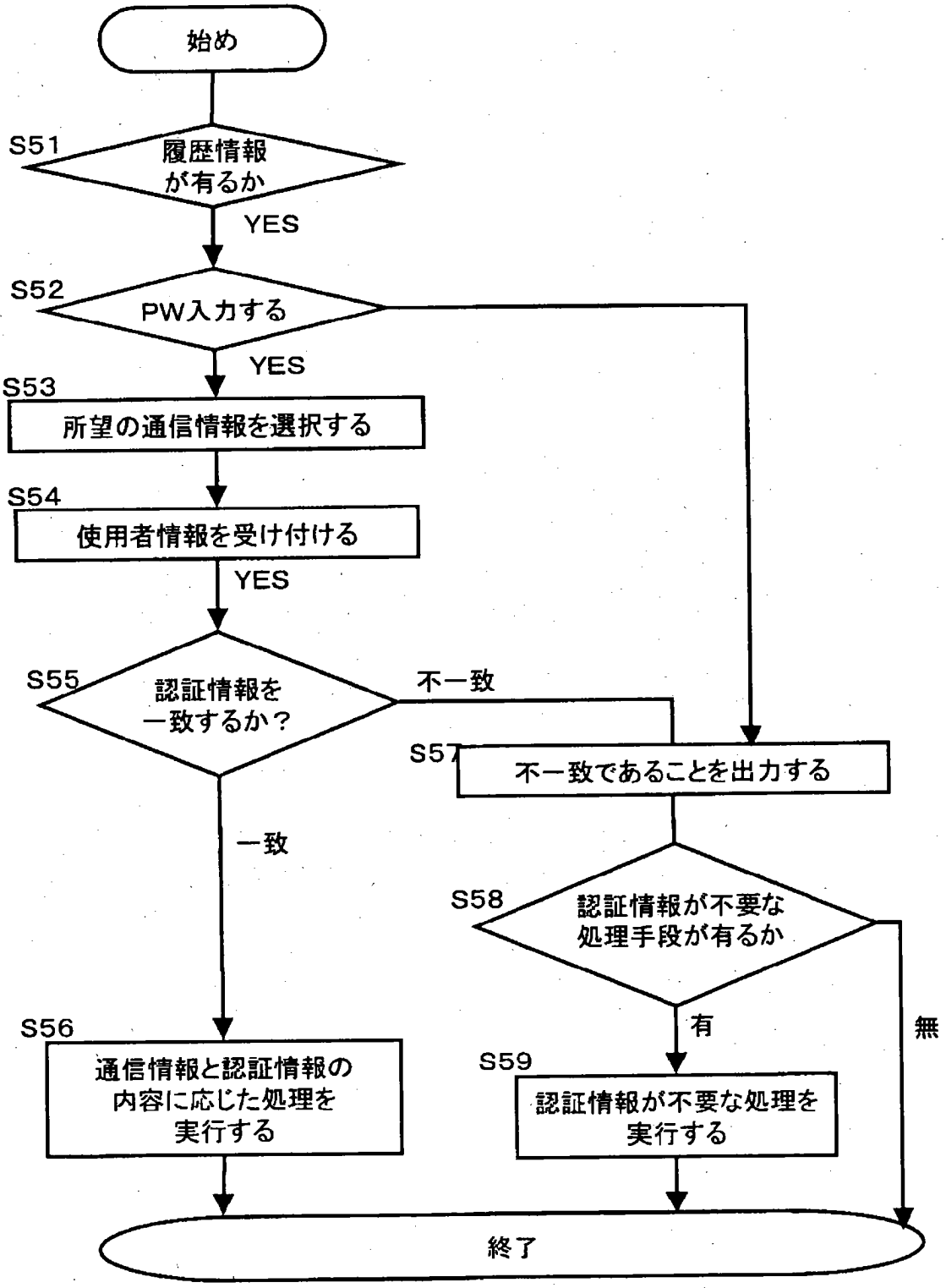
【図１２】


602
Vdd
603
R 605
INS 604
622
検出部
628
履歴情報
記録部
624
履歴
情報
626
コントローラー
Vss
606
300C
308
制御部
312
認証部
315
処理部
408
選択部
305
受付部
305
記憶部
306
第1記憶部
314
第2記憶部
405
第4記憶部
303
設定部
320
認証情報設定部
322
処理手段設定部
410
通信情報設定部

【図１３】


始め
S41
検出部がＩＮＳを
受信する
S42
ＩＮＳを履歴情報
記録部に送信する
S43
ＩＮＳを履歴情報として
履歴情報記録部に
記録する
終了

【図１４】


始め
S51
履歴情報が有るか
YES
S52
PW入力する
YES
S53
所望の通信情報を選択する
S54
使用者情報を受け付ける
YES
S55
認証情報を一致するか？
不一致
S57
不一致であることを出力する
一致
S58
認証情報が不要な処理手段が有るか
有
無
S56
通信情報と認証情報の内容に応じた処理を実行する
S59
認証情報が不要な処理を実行する
終了

【書類名】　要約書

【要約】

【課題】　端末装置に着脱可能な記録媒体の不正使用を防止し、かつ利便性の高い記録媒体不正使用防止システムを提供する。

【解決手段】　端末装置に着脱可能な記録媒体の不正使用防止システムは、記録媒体の使用の可否を決定する認証情報を複数記憶する第１記憶部と、第１記憶部に記憶された認証情報に対応した処理手段を記憶する第２記憶部と、端末装置の通信機能を使用するための通信情報を複数記憶する第４記憶部と、第４記憶部の通信情報から所望の通信情報を選択する選択部と、記録媒体の使用者が有する使用者情報と認証情報との認証を行う認証部と、選択部により選択された通信情報と認証部の認証の内容とに対応した処理手段を実行する処理部と、を備える。

【選択図】　図９

出願人履歴情報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社